What is claimed is:

1. A digital communication system to denote confidentiality of a digital communication comprising:

a processor; and,

a memory containing a program executable by the processor to:

attach a privileged attribute to a digital communication;

create a privileged distribution list of at least one intended recipient;

restrict access to the privileged digital communication to the at least one intended recipient;

restrict routing of the privileged digital communication to the at least one intended recipient; and,

store the privileged digital communication in a segregated location on a data storage device.

2. The communication system of claim 1, wherein the at least one intended recipient is a plurality of intended recipients.

3. The communication system of claim 1 further comprising:

a mail server; and,

a segregated server housing the segregated location;

wherein the program is further executable to send a copy of the communication to the segregated server.

4. The communication system of claim 3, wherein the copy is sent as a blind carbon copy.

5. The communication system of claim 1 wherein the segregated location is divided by a common characteristic of the digital communication, the common characteristic including:

a sender of the digital communication;

a recipient of the digital communication; and,

a department of a corporation using the system.

6. The communication system of claim 1 wherein the program is further executable to configure access rights to the digital communication and to enforce said access rights by managing access to the digital communication and controlling the manipulation of its contents.

7. The communication system of claim 6 wherein the access rights include:

forwarding of the communication;

replying; and

replying with copies to pre-selected recipients.

8. The communication system of claim 6 wherein the communication includes an address portion and a content portion, and wherein the access rights further include:

allowing copying of the contents of the communication; and

allowing cutting the contents of the communication out of the communication and pasting the cut out contents into another location.

9. The communication system of claim 1 wherein the program is configured to execute automatically and attach the privileged attribute to particular communications according to pre-determined selection criteria.

10. The communication system of claim 1 further comprising a confidentiality notice that is displayed to a user and acknowledged by the user before displaying the privileged communication.

11. The communication system of claim 10 wherein the user acknowledges the confidentiality notice by clicking on a GUI button.

12. The communication system of claim 1 wherein the privileged digital communication is encrypted.

13. The communication system of claim 1 wherein the program further comprises a server object and a client object.

14. The communication system of claim 13 wherein the client object is configured to attach the privileged attribute, create the privileged distribution list and send the privileged communication to the server object.

15. The communication system of claim 13 wherein the server object restricts access and routing of the digital communication and stores the communication in the segregated location.

16. The communication system of claim 13 wherein the client object is a plug-in to a pre-existing communication system.

17. The communication system of claim 1 further comprising a second segregated location residing on a client device.

18. A digital communication system for denoting confidentiality of a digital communication comprising:

a processor; and,

a memory containing a program executable by the processor to:

attach an executable module to a digital communication, the executable module constructed and arranged to:

create a privileged distribution list of intended recipients of the digital communication;

restrict access to the digital communication to the intended recipients;

restrict routing of the digital communication to the intended recipients.

19. The communication system of claim 18 wherein the program is further executable to configure access rights to the digital communication and to enforce said access rights by managing access to the digital communication and controlling the manipulation of its contents, wherein the access rights include:

allowing forwarding of the communication;

allowing replying; and

allowing replying with carbon copies to pre-selected recipients.

20. The communication system of claim 18 wherein the communication includes an address portion and a content portion, and wherein the access rights further include:

allowing copying of the contents of the communication;

allowing cutting the contents of the communication out of the communication and pasting the cut out contents into another location;

21. The communication system of claim 18 wherein the program is configured to execute automatically and attach the executable module to particular communications according to predetermined selection criteria.

22. The communication system of claim 18 further comprising a confidentiality notice that is displayed to a user and acknowledged by the user before displaying the privileged communication.

23. The communication system of claim 18 wherein the privileged digital communication is encrypted.

24. The communication system of claim 18, wherein the program further comprises a server object and a client object.

25. The communication system of claim 23 wherein the client object is configured to attach the executable module, and send the privileged communication to the server object.

26. The communication system of claim 23 wherein the server object restricts access and routing of the digital communication and stores the communication in a segregated location.

27. The communication system of claim 23 wherein the client object is a plug-in to a pre-existing communication system.

28. A privileged e-mail messaging system, comprising:
an executable module, the executable module configured to instruct a computer to maintain confidentiality of an e-mail message to which the executable module is attached by restricting access to the e-mail message to a privileged distribution list of intended recipients, restricting routing of the e-mail message to the intended recipients in the privileged distribution list, and by managing manipulation of its contents; and
an e-mail messaging system, the e-mail messaging system configured to create an e-mail message and to transmit the e-mail message, the e-mail messaging system attaching the executable module to the e-mail message prior to transmission.

29. The system according to claim 28, wherein the executable module is configured to execute when the e-mail message is opened, the executable module granting access to the message during said execution if a predetermined condition is met.

30. The system according to claim 29 wherein the predetermined condition is a user being in the privileged distribution list.

31. A digital communication system to denote confidentiality of a digital communication comprising:

a processor;

a memory connected to the processor, the memory containing:

a program including:

a container creator utility to create a virtual container and place a privileged digital communication in the container; and

a container opener utility to open the virtual container and remove the privileged digital communication.

32. The communication system of claim 31 wherein the program is further executable to configure access rights to the digital communication and enforce said access rights by managing access to the digital communication and controlling the manipulation of its contents, the access rights including:

allowing forwarding of the communication;

allowing replying; and

allowing replying with carbon copies to pre-selected recipients.

33. The communication system of claim 32 wherein the communication includes an address portion and a content portion, and wherein the access rights further include:

allowing copying of the contents of the communication;

allowing cutting the contents of the communication out of the communication and pasting the cut out contents into another location.

34. The communication system of claim 31 wherein the program is configured to execute automatically and attach the executable module to particular communications according to predetermined selection criteria.

35. The communication system of claim 31 further comprising a confidentiality notice that is displayed to a user and acknowledged by the user before displaying the privileged communication.

36. The communication system of claim 31 wherein the privileged digital communication is encrypted.

37. The communication system of claim 31 wherein the program further comprises a server object with the container opener and a client object with the container creator.

38. The communication system of claim 37 wherein the client object is a plug-in to a pre-existing communication system.

39. The virtual container system of claim 31 wherein the container creator utility is further executable to :

create a virtual container which resides in contiguous locations in an electronic storage media of a computer, wherein the virtual container includes a header portion and a digital object portion;

receive a digital object selection and a privilege profile from a user;

apply an encryption technique to the selected digital object to create an encrypted digital object;

write the encrypted digital object into the digital object portion of the virtual container; and,

write information indicative of the privilege profile into the header portion of the virtual container.

40. The virtual container system of claim 31 wherein the container opener utility is further executable to :

read the information indicative of the privilege profile from the header portion of the virtual container;

determine, based upon said information, if access to the digital object should be granted to a user;

read the encrypted digital object from the digital object portion; and,

apply a decryption technique to the digital object if the user is privileged as a function of the privilege profile.

41. A method for creating an attorney-client privileged digital communication comprising the steps of:

creating an electronic communication;

marking the communication privileged with a privileged attribute;

storing the communication in a segregated location on a data storage device;

configuring access rights to the digital communication; and,

enforcing said access rights by managing access to the digital communication and controlling the manipulation of its contents;

wherein the access rights include:

forwarding of the communication;

replying; and

replying with copies to pre-selected recipients.

42. The method of claim 41 wherein the communication includes an address portion and a content portion, and wherein the access rights include:

copying of the contents of the communication;

cutting the contents of the communication out of the communication and

pasting the cut out contents into another location.

43. The method of claim 41 further comprising automatically attaching the privileged attribute to particular communications according to pre-determined selection criteria.

44. The method of claim 41 further comprising:

displaying a confidentiality notice to a user; and,

requiring acknowledgment by the user of the confidentiality notice before displaying the privileged communication.

45. The method of claim 41 further comprising applying an encryption technique to the digital communication.

46. The method of claim 41 further comprising the steps of:

creating a blind carbon copy of the digital communication;

sending the blind carbon copy to a segregated server wherein the segregated location resides on the segregated server.

47. The method of claim 41 further comprising dividing the segregated location by a common characteristic of the digital communication, the common characteristic including one or more of:

a sender of the digital communication;

a recipient of the digital communication; and

a department of a corporation.

48. The method of claim 41 further comprising the steps of:

creating a second segregated location on a client device;

storing a copy of the digital communication on the second segregated location.

49. A method for creating a digital communication protected by privilege comprising the steps of:

creating an executable module constructed and arranged to instruct a

computer to restrict access to the communication to which the executable module is attached in order to maintain the application of the privilege;

attaching the executable module to the communication.

50. The method of claim 49 further comprising:

configuring access rights to the digital communication;

enforcing said access rights by managing access to the digital communication and controlling the manipulation of its contents.

51. The method of claim 49 wherein the access rights include:

forwarding the communication;

replying; and

replying with carbon copies to pre-selected recipients.

52. The method of claim 49 wherein the communication includes an address portion and a content portion, and wherein the access rights include:

copying of the contents of the communication;

cutting the contents of the communication out of the communication and pasting the cut out contents into another location.

53. The method of claim 49 further comprising a privilege profile, the profile containing the privileged distribution list and the access rights.

54. The method of claim 49 wherein the program is configured to execute automatically and attach the executable module to particular communications according to predetermined selection criteria.

55. The method of claim 49 further comprising a confidentiality notice that is

displayed to a user and acknowledged by the user before displaying the privileged communication.

56. The method of claim 49 further comprising applying an encryption technique to the digital communication.

57. A method for creating a privileged digital document, comprising the steps of:

creating an executable module which instructs a computer to maintain confidentiality in communication of the privileged digital document to which the executable module is attached by restricting access to the digital document and managing manipulation of its contents;

attaching the executable module to the document.

58. The method according to claim 57, further comprising the step of executing the executable module when the document is opened.

59. The method of claim 57, wherein the document is an encrypted document, and wherein the executable module is configured to instruct the computer to decrypt the document if a predetermined condition is met.

60. A method for creating a digital communication protected by the attorney-client privilege comprising the steps of:

creating a virtual container, the virtual container residing in contiguous locations in an electronic storage media of a computer, the virtual container including a header portion and a digital object portion;

selecting a digital communication for insertion into the virtual container;

applying an encryption technique to the digital communication to create an encrypted digital communication;

writing the encrypted digital communication into the digital object portion;

creating a privilege profile for the digital object, the privileged profile including a list of intended recipients and specific actions each of the recipients may take on the digital communication;

writing information indicative of the privilege profile into the header portion of the virtual container;

configuring access rights to the digital communication; and,

enforcing said access rights by managing access to the digital communication and controlling manipulation of its contents;

wherein the access rights include:

forwarding the communication;

replying; and

replying with carbon copies to pre-selected recipients.

61. The method of claim 59 wherein the communication includes an address portion and a content portion, and wherein the access rights include:

copying the contents of the communication;

cutting the contents of the communication out of the communication and pasting the cut out contents into another location.

62. The method of claim 60 further comprising the step of automatically attaching the executable module to particular communications according to predetermined selection criteria.

63. The method of claim 60 further comprising a confidentiality notice that is displayed to a user and acknowledged by the user before displaying the privileged communication.

64. The method of claim 60 further comprising applying an encryption technique to the digital communication.

65. A method for creating a virtual container and extracting a digital object from a virtual container, wherein the method of creating the virtual container comprises the steps of :

creating a virtual container, the virtual container residing in contiguous locations in an electronic storage media of a computer, the virtual container including a header portion and a digital object portion;

selecting a digital object for insertion into the virtual container;

applying an encryption technique to the digital object to create an encrypted digital object;

writing the encrypted digital object into the digital object portion;

configuring a privilege profile for the digital object, the privilege profile containing a list of intended recipients and the actions each one of the intended recipients may take on the digital object; and

writing information indicative of the privilege profile into the header portion of the virtual container;

and wherein the method for extracting the document from the virtual container, comprises the steps of :

reading information indicative of the privilege profile from a header portion of a virtual container,

determining, based upon said information, if a user is privileged to access contents of the digital object and to manipulate the contents as defined by the privilege profile;

restricting access to the object if the user is not privileged; and

reading the digital object from the digital object portion and applying a decryption technique to the digital object if the user is privileged.

66. The method of claim 65, wherein the step of creating the virtual container includes the step of creating a container header and an digital object header, the container header containing information regarding the container including a container name, the digital object header containing information regarding the digital object including a name of the digital object.

67. The method of claim 65, wherein the step of writing information indicative of the expiration date includes writing said information into the container header.

68. The method of claim 65, wherein

the step of selecting a digital object for insertion into the virtual container includes selecting a plurality of digital objects for insertion into the virtual container;

the step of applying an encryption technique includes applying the encryption technique to each of the plurality of digital objects;

the step of writing the encrypted digital object into the digital object portion includes writing each of the encrypted digital objects into the digital object portion;

the step of selecting an expiration date includes selecting an expiration date for each of the plurality of digital objects; and

the step of writing information includes writing the information indicative of the privilege profile of each one of the digital objects into a respective digital object header.

69. The method of claim 65 further comprising

transmitting the virtual container and a container opener utility to a recipient, wherein the container opener utility, when invoked by the recipient, reads the information indicative of the privilege profile from the header portion of the virtual container, determines, based upon said information, if the recipient is privileged to access the digital object, denies access if the recipient is not privileged, and reads the encrypted digital object from the digital object portion and applies a decryption technique to the digital object if the user is

privileged.

70. The method of claim 65, wherein the virtual container is transmitted via the Internet.

71. A digital communication system to comprising:

a processor; and,

a memory containing a program executable by the Processor to:

attach a privileged attribute to a digital communication;

restrict access to the privileged digital communication to an intended recipient and the pre-registered designees of attorney recipients; and

store the privileged digital communication in a segregated location on a data storage device.

72. A digital communication system comprising:

a processor; and,

a memory containing a program executable by the processor to:

attach an executable module to a digital communication, the executable module constructed and arranged to:

restrict access to the digital communication to an intended recipient and pre-registered designees of attorney recipients;

restrict routing of the digital communication to the intended recipient and pre-registered designees of attorney recipients.